Washington Journal of Law, Technology & Arts

Volume 7 | Issue 1 Article 2

7-1-2011

# Broadcasting Expectations: An Unprotected Wireless Network Takes on Constitutional Dimensions

Duncan Stark

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 1 SUMMER 2011

# BROADCASTING EXPECTATIONS: AN UNPROTECTED WIRELESS NETWORK TAKES ON CONSTITUTIONAL DIMENSIONS

*Duncan Stark*[*]


Cite as: 7 Wash J.L. Tech. & Arts 1 (2011)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1048

## ABSTRACT

*In January 2010, the U.S. District Court for the District of Oregon decided* U.S. v. Ahrndt*, the first case regarding the reasonable expectation of privacy in a home wireless internet network. The court found that the defendant had no reasonable expectation of privacy in his unsecured home wireless network because he had openly shared information on a system freely accessible by his neighbors. This Article examines the* Ahrndt *case and the potential legal effect this issue may have on an individual's expectation of privacy in his or her wireless network and personal computer files. This Article concludes that although the exact effects of new technologies on search and seizure law have not been fully explored by the courts, people should not expect the courts to consider unencrypted wireless networks to be private.*

[*] Duncan Stark, University of Washington School of Law, Class of 2012. Thank you to Professor Anita Ramasastry of the University of Washington School of Law, student editor Caitlin Steiger, and Floyd Short of Susman Godfrey L.L.P. for their guidance.

## TABLE OF CONTENTS



## INTRODUCTION

Defendant John Henry Ahrndt, on trial for transportation and possession of child pornography, challenged the admissibility of key evidence based on the fact that the materials were discovered on his computer through his home wireless network by a police officer without a warrant.[1] In the first case of its kind, the U.S. District Court for the District of Oregon found that Ahrndt could not have had a reasonable expectation of privacy in files he shared openly on an unsecured wireless network, preventing his claim that the officer violated the Fourth Amendment.[2]

This Article discusses the extent of protections against searches and seizures under the Fourth Amendment, discusses the new issues raised by the *Ahrndt* case, and explores possible future cases that may present similar issues. This Article also analyzes cases arising out of related new technologies to determine their potential influence on the law of search and seizure and the legality of searching computer networks.

---

[1] United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *1 (D. Or. Jan. 28, 2010).

[2] *Id.* at *9.

## I. FOURTH AMENDMENT FRAMEWORK: AN EMPHASIS ON REASONABLENESS

The Fourth Amendment provides citizens with the right to be secure from unreasonable government searches and seizures of their persons, houses, papers and effects.[3] The Amendment provides no protection against searches performed by private citizens,[4] and it has been established that invasions of a defendant's privacy by governmental agents subsequent to invasions by a private party are tested by the degree to which they exceed the scope of the private search.[5]

The United States Supreme Court decision in *Katz v. United States* introduced a two-part test for determining whether a court-issued warrant is required for a search or seizure.[6] First, a person must subjectively expect privacy in the thing searched, and second, society must recognize this expectation as reasonable.[7] The cases discussed in this Article, in general, turn on the second prong of this test: whether the expectation of privacy is one society accepts as reasonable.

In applying this standard to specific situations, the Supreme Court has taken a case-by-case approach. However, some trends emerge from an analysis of the relevant cases.[8] For example, the Court has recognized that developments in technology have served to decrease reasonable expectations of privacy.[9]

In *Rakas v. United States*, the Court articulated a standard that is often applied by lower courts to evaluate whether a reasonable

---

[3] U.S. CONST. amend. IV.

[4] United States v. Jacobson, 466 U.S. 109, 113 (1984).

[5] *Id.* at 115.

[6] Katz v. United States, 389 U.S. 347 (1967) (finding that investigators violated a suspect's reasonable expectation of privacy when they listened to a conversation inside a telephone booth using a wiretap).

[7] *Id.* at 361 (Harlan, J., concurring).

[8] THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 64-65 (Carolina Academic Press 2008).

[9] *Id.* at 65. *See also* California v. Ciraolo, 476 U.S. 207, 215 (1986) ("[i]n an age where private and commercial flight in the public airways is routine," there is no reasonable expectation of privacy from 1,000 feet in the air).

expectation of privacy exists in a given situation.[10] In that case, the Court stated that "legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[11] Ninth Circuit precedent provides further guidance by establishing factors to help courts determine whether a reasonable expectation of privacy exists. These include the defendant's possessory interest in the thing searched,[12] the measures the defendant took to protect it,[13] whether it was labeled as private,[14] and the presence or absence of a right to exclude others.[15] With this framework in mind, the remainder of this Article discusses the novel issue of whether Fourth Amendment protections extend to an unsecured wireless network.

## II. DISTRICT COURT FINDS NO REASONABLE EXPECTATION OF PRIVACY IN UNSECURED WIRELESS NETWORKS

John Henry Ahrndt was convicted of transportation and possession of child pornography in violation of federal law based on evidence found on his computer through his wireless network.[16] In February 2007, an Oregon resident identified as JH was using her personal computer when it automatically picked up a nearby wireless network, to which she connected.[17] JH began using Apple's iTunes software, which allows users to share media files such as digital photos and music over computer networks, and noticed that another user's files were available to her over the wireless network.[18] After reading the names of some of these files, JH realized that they contained child pornography and contacted the Washington County

[10] Rakas v. Illinois, 439 U.S. 128 (1978).
[11] *Id.* at 143 n.12.
[12] United States v. Broadhurst, 805 F.2d 849, 851 n.2 (9th Cir. 1986).
[13] *Id.*
[14] *Id.*
[15] United States v. Bautista, 362 F.3d 584, 589 (9th Cir. 2004).
[16] He was convicted of violating 18 U.S.C. §§ 2252-2253 (2006).
[17] U.S. v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *1 (D. Or. Jan. 28, 2010).
[18] *Id.*

Sheriff's Office.[19] Further police investigation, including using the computer belonging to JH to connect to the wireless network, using her computer's iTunes software to access the files in question, and opening one of the files, revealed that the files indeed contained child pornography and that the network and the files were those of the defendant.[20]

At trial, Ahrndt filed a motion to suppress the evidence obtained through his wireless network, arguing that it was the product of a search that violated his Fourth Amendment rights.[21] The district court found that Ahrndt did not demonstrate a subjective expectation of privacy, and that even if he had, such an expectation was unreasonable because he had left his wireless network unencrypted and his iTunes settings openly shared his files with that network.[22]

In support of his Fourth Amendment argument, Ahrndt also claimed that the files had been part of an electronic communication protected by the Electronic Communications Privacy Act (ECPA), which he said provided evidence that his expectation of privacy in those files was reasonable.[23] The ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Federal Wiretap Act). It protects against the interception of electronic communications, including those stored on a computer, and establishes the legal standards the government must satisfy to obtain stored or real-time electronic communications.[24] The court found, however, that the access was expressly authorized under ECPA because the evidence was obtained "through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[25]

---

[19] *Id.*
[20] *Id.* at *2.
[21] *Id.*
[22] *Id.* at *5.
[23] *Id.* at *7.
[24] 18 U.S.C. § 2511 (2006). *See also Ahrndt*, 2010 WL 373994, at *8.
[25] *Ahrndt*, 2010 WL 373994, at *8 (quoting 18 U.S.C. § 2511 (2006)).

## III. IMPLICATIONS FOR PRIVACY IN SECURED AND UNSECURED WIRELESS NETWORKS

As wireless networking technology becomes increasingly ubiquitous, cases similar to *Ahrndt* will likely arise. Variations on the facts of this case may lead to more difficult constitutional questions. As the Supreme Court stated in *City of Ontario v. Quon*, a case in which a municipal employer searched the contents of an employee's city-issued pagers, "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[26] Emerging technologies such as wireless networks, data encryption, and file-sharing networks are likely to raise issues in regard to their potential effects on the legality of searches.

### A. *Expectation of Privacy in Wireless Communications*

Courts have held that people have lower expectations of privacy in wireless communications because of the ease with which information can be intercepted. Yet legislation may provide protection where the Constitution does not. The seminal case on this issue is the 1973 decision in *United States v. Hall*, in which defendant-appellant Hall was convicted after using radio telephones that had been installed in his car to call landline phones to distribute marijuana.[27] Hall argued that evidence obtained by intercepting the radio calls was the fruit of an illegal search.[28] The court stated that conversations intercepted in this manner theoretically should not be afforded more protection than one between two radio transceivers. But the Ninth Circuit explained that it was constrained by the language of the Federal Wiretap Act to find that Hall's communication was protected by that statute, which defined "wire communication" as any transfer "made in whole or in part through" wire, cable, or other like connection, where one end of the phone call was made on a landline.[29]

---

[26] City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).
[27] United States v. Hall, 488 F.2d 193, 194 (9th Cir. 1973).
[28] *Id.*
[29] *Id.* at 196-97. *See also* 18 U.S.C. § 2510 (2006).

The *Hall* court's reasoning prevailed in the later decision *Tyler v. Berodt*.[30] In that case, the Berodt family listened to conversations the Tylers made using a cordless phone connected to their landline service. After overhearing conversations that led them to suspect criminal activity, the Berodts alerted the police.[31] In the ensuing civil suit against the Berodts and law enforcement officers, the court was unconstrained by the Federal Wiretap Act because the 1986 amendment by the ECPA changed the definition of "wire communication" to exclude the radio portion of a phone call carried in part over a wire.[32] The *Berodt* court held that because there was no reason for the Tylers to expect privacy in conversations using such a device, those conversations were not protected by the Fourth Amendment.[33] Other courts have found that the wireless portions of phone calls also transmitted in part over landlines are not protected by the Fourth Amendment.[34] In 1994, however, the Federal Wiretap Act was amended again to protect wireless communications.[35]

The *Hall* and *Berodt* cases illustrate that courts generally find that wireless communications, especially those using radio frequency technology, do not give rise to an expectation of privacy. This is based on the fact that radio frequency communications are easily intercepted, and a belief that people are generally aware (or should be aware) of this fact.

### *B. Password Protection*

While courts afford less Fourth Amendment protection to wireless communications, they have determined that people do have a reasonable expectation of privacy in their personal computer files,

---

[30] Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989).

[31] *Id.* at 705-06.

[32] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(a), 100 Stat. 1848 ("such term [wire communications] does not include the radio portion of a cordless telephone [call] that is transmitted between the cordless telephone handset and the base unit").

[33] *Berodt*, 877 F.2d at 706-07.

[34] *See, e.g.*, United States v. Hoffa, 436 F.2d 1243, 1247 (7th Cir. 1970); Edwards v. Bardwell, 632 F.Supp. 584, 589 (M.D. La. 1986); State v. DeLaurier, 488 A.2d 688, 694 (R.I. 1985).

[35] *See, e.g.*, McKamey v. Roach, 55 F.3d 1236, 1240-41 (6th Cir. 1995).

especially where the files are password protected. In *U.S. v. Heckenkemp*, the Ninth Circuit held that a student had a reasonable expectation of privacy in his computer's files despite having used the computer to hack into the university's e-mail system.[36] In an appeal from his conviction for intentionally accessing a protected computer without authorization based in part on evidence collected from his computer, the court stated that "he also had a legitimate, objectively reasonable expectation of privacy in his personal computer," and that "the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer."[37] The court found the search justified on other grounds.[38]

A person may lose any expectation of privacy achieved by using a password by sharing it with others. In *U.S. v. D'Andrea*, the defendant and her boyfriend had allegedly sexually abused the defendant's eight-year-old daughter and posted pictures of the abuse to a password-protected website.[39] An anonymous caller to the Department of Social Services reported the activity and provided the password.[40] At trial, D'Andrea challenged the introduction of the photos based on her expectation of privacy in them.[41] The United States District Court for the District of Massachusetts held that the password protection did convey an expectation of privacy, but because she had shared the password to the site with another person, she had assumed the risk that it would be exposed.[42]

The absence of password protection has also been cited as a reason to find that there was not a reasonable expectation of privacy in digital files. For example, in *Casella v. Borders*, a woman lent her phone to her boyfriend, who was subsequently arrested.[43] A police officer discovered sexual photos of the couple on the phone and disclosed them publicly.[44] In the resulting suit for emotional distress

[36] United States v. Heckenkemp, 482 F.3d 1142, 1147 (9th Cir. 2007).
[37] *Id.* at 1146-47.
[38] *Id.* at 1147.
[39] United States v. D'Andrea, 497 F.Supp.2d 117, 118 (D. Mass. 2007).
[40] *Id.*
[41] *Id.* at 119.
[42] *Id.* at 123.
[43] Casella v. Borders, 649 F.Supp.2d 435, 437 (W.D. Va. 2009).
[44] *Id.* at 473.

and Fourth Amendment violations, the United States District Court for the Western District of Virginia dismissed her claims because she had taken no measures to protect the images, specifically citing the absence of password protection on the phone.[45]

### C. *Distinguishing* Ahrndt

Even with the *Ahrndt* decision as precedent, a defendant may have a reasonable expectation of privacy in computer files that he or she did not intend to be shared on even an unencrypted network. In *Ahrndt*, JH would not have stumbled across Ahrndt's files had he not openly shared them on that network through his iTunes software.[46] The holding in this case was thus only that Ahrndt had no reasonable expectation of privacy in files shared on an unsecured wireless network.[47] In the words of the court, "in order to hold that defendant had no right to privacy, it is also necessary to find that society would not recognize as reasonable an expectation of privacy in the contents of a shared iTunes library available for streaming on an unsecured wireless network." This is a factual distinction that may make a difference in future cases.

### *D. Restrictions on Unauthorized Network Access*

One additional point on the nature of wireless networking could be a potential factor in future cases: state and federal laws prohibit accessing a computer network without authorization. For example, Oregon makes accessing a computer without authorization a Class A misdemeanor, and Washington makes accessing a computer system without authorization a gross misdemeanor.[48] The federal Computer Fraud and Abuse Act also criminalizes the unauthorized access of

---

[45] *Id.* at 439.

[46] *See* United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *5 (D. Or. Jan. 28, 2010) (explaining that the default setting in the iTunes software in question was not to share files on the network, indicating that he took affirmative action to make the files public).

[47] *Ahrndt*, 2010 WL 373994, at *5-7.

[48] OR. REV. STAT. § 164.377 (2009) (making "Computer Crime" a Class A misdemeanor); WASH. REV. CODE § 9A.52.120 (2010) (making "Computer Trespass in the Second Degree" a gross misdemeanor).

computer networks in some circumstances.[49] If these statutes reflect societal expectations about privacy, the illegal nature of these actions arguably suggest that society is prepared to afford even unsecured wireless networks a reasonable expectation of privacy. Ahrndt did not argue and the court did not consider this point, perhaps because, though illegal, the practice of accessing open wireless networks is common and possibly even accepted.[50]

### *E. Reduced Privacy Expectations in File-Sharing Networks*

As courts have reduced the reasonable expectation of privacy in wireless communications, they have also reduced such expectations in the context of file-sharing networks. In two Ninth Circuit cases on the issue, the court held that a police officer who accessed child pornography on a defendant's computer through the LimeWire file-sharing network was not burdened by the prohibitions of the Fourth Amendment.[51] In *U.S. v. Ganoe*, the court held that the defendant "knew or should have known that the software might allow others to access his computer,"[52] and that "[m]oreover, he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network."[53]

The defendant in *U.S. v. Borowy*, a case with very similar facts, attempted to distinguish *Ganoe* by arguing that the defendant had specifically downloaded a version of the software with an option (which he attempted to engage) that could block others from accessing his files.[54] The court held he had no reasonable expectation of privacy in his files available to LimeWire because he had downloaded and used software that he knew would allow others to

---

[49] 18 U.S.C. § 1030 (2006).

[50] *See* Randy Cohen, *The Ethicist: Wi-Fi Fairness*, N.Y. TIMES (Feb. 8, 2004), http://wwnytimes.com/2004/02/08/magazine/08ETHICIST.html (arguing that it is ethical to "use but not overuse Wi-Fi hot spots you encounter").

[51] *See* United States v. Ganoe, 538 F.3d 1117, 1119 (9th Cir. 2008), *cert. denied*, 129 S.Ct 2037 (2009); United States v. Borowy, 595 F.3d 1045, 1046 (9th Cir. 2010).

[52] *See Ganoe*, 538 F.3d at 1117.

[53] *See Ganoe*, 538 F.3d at 1127.

[54] *Borowy*, 595 F.3d at 1047.

view his files and had failed to take the steps necessary to prevent others from doing so.[55]

This recent case law illustrates that with both wireless and file-sharing networks, users often set up hardware and software with default settings, typically leaving the networks open to the public despite warnings that there are steps that can be taken to protect the data. This practice appears to reduce the amount of privacy that users can expect in these networks.

## CONCLUSION

The *Ahrndt* case is the first to deal with expectations of privacy in wireless networks, but it likely represents the first case of many to raise these sorts of constitutional questions. New technologies generally decrease the amount of privacy people have in their persons, houses, papers and effects, and the courts have begun to outline some of the contours of this area of the law. Wireless communications generally cannot be expected to be private. Encrypted or password-protected digital files, however, can generally be expected to be private. Finally, where a person exposes his or her computer or files to the world, as most file-sharing network users (and many wireless-network users) do, he or she loses any expectation of privacy in the files. The *Ahrndt* decision is consistent with prior law and signals a sensible rule going forward.

[55] *Id.* at 1048.